COMPUTING SECURITY:

FEATURES IN THE SEPTEMBER-OCTOBER 2022 ISSUE

YOUR CHANCE TO CONTRIBUTE...

We are looking for **300-400 words** of expert commentary on one of the below features, delivered to editor Brian Wall by email – bp.wall@btinternet.com – on or before **THE DEADLINE DATE SHOWN BELOW**.

GUIDELINES – THESE APPLY TO ALL SUBMISSIONS:

Submissions must be based on the synopsis provided and may need to be edited down where space does not allow the submission to run in full and also where contributions from several sources overlap.

The submission should come from a named spokesperson within the company, with full job title and **HIGH-RESOLUTION** image, plus any other relevant HIGH-RES 'action' shots.

Also, it is essential that the copy should be editorial – and therefore neutral – in tone, specifically addressing the issues raised in the synopses above. If it is not editorial in style and content, nor in synch with the synopsis, it is unlikely to be used.

If you would like to be involved, please contact me as soon as possible at the email address shown above, so I can allocate space. This will be strictly limited for all features.

PLEASE SPECIFY IN THE EMAIL WHICH FEATURE THE CONTRIBUTION WILL BE FOR.

THE DEADLINE FOR ALL SUBMISSIONS IS FRIDAY, 12 AUGUST, 2022

MAIN FEATURES SYNOPSES...

RANSOMWARE DEMAND? – 'DON'T PAY IT!'

In a letter to the Law Society, the National Cyber Security Centre (NCSC) – which is a part of GCHQ – and Information Commissioner's Office (ICO) state that they have seen evidence of a rise in ransomware payments and that, in some cases, solicitors may have been advising clients to pay, in the belief that it will keep data safe or lead to a lower penalty from the ICO. They have asked the Law Society to remind its members of their advice on ransomware and emphasise that paying a ransom will not keep data safe or be viewed by the ICO as a mitigation in regulatory action.

How sound is this advice and should anyone hit by ransomware follow it without exception? What if your organisation faces possible meltdown from such an attack, unless it can get its systems back up and running – and fast? Most importantly, for those who have never yet been a victim, is a ransomware attack bound to succeed, if you are targeted, or are their 'foolproof' ways to stay protected?

BREACHES '80% DOWN TO HUMAN FAILURES'

Human error remains a major root cause of data breaches, a new report has found. Verizon's annual Data Breach Investigations Report for 2022 revealed that human elements such as social engineering and misuse of privileged access were a factor in more than four out of five breaches.

How can organisations get control over what has often been branded 'the enemy within' – their own people? What controls need to be put in place to prevent such abuses happening in the workplace? Are there any 'failsafe' systems that can be implemented or it mostly about damage limitation? How can employee behaviour be better monitored without alienating the very people on whom these organisations rely for their success?

MALWARE MANIA

Attackers are using and re-using malware that has been proven to deliver results. They're doing this as part of a larger, orchestrated attack chain, according to new research from Cisco. Two major reasons for their success are: their ability to deploy follow-up malware that does further damage down the cyber-attack chain; their highly distributed command-and-control (C2) infrastructure makes take-down harder.

We ask the experts if predictive threat intelligence can help to counter these rising trends and how the technology works. Do different predictive threat intelligence solutions take varying approaches? If so, what are the options available and what do they deliver? Also, are such solutions right for all organisations, irrespective of industry focus or size? Are they expensive to purchase and implement? What are the on-going cost implications? And are there sound alternative technologies that do as good, or better, a job?

THE FLAMES OF DISCONTENT

It's extremely rare for hackers, who almost exclusively operate in the digital world, to cause damage in the physical world. But a cyber-attack on a steel maker in Iran recently, reported by the BBC, is being seen as one of those significant and troubling moments.

A hacking group called Predatory Sparrow said it was behind the attack, which it said caused a serious fire and released a video to back up its story. The video appears to be CCTV footage of the incident, showing factory workers leaving part of the plant before a machine starts spewing molten steel. It ends with people pouring water on the fire with hoses.

Has hacking taken on a much more sinister role, targeting groups, individuals and even national interests for their personal and/or political convictions? How widespread are such attacks now and are we likely to see these escalate? If so, are those charged with preventing such extreme actions up against insurmountable odds in trying to track down and apprehend these invisible foe?

IOT – INSTRUMENTS OF THREAT?

It is estimated that, by 2026, there will be 64 billion IoT devices installed around the world, according to Kaspersky, with the trend towards remote working helping to drive this increase. "So many additional devices change the dynamics and size of what is sometimes called the cyber-attack surface – that is, the number of potential entry points for malicious actors," the company reports. Compared to laptops and smartphones, most IoT devices have fewer processing and storage capabilities. "This can make it harder to employ firewalls, antivirus and other security applications to safeguard them."

Will these attacks get more sophisticated and frequent? What are the worst-case scenarios that organisations are going to face in an IoT device saturated workspace? How can all of the security

risks that go with IoT devices be controlled? Does this signal how our ability to defend against attacks is, inevitably, becoming a losing battle?

IF CONTRIBUTORS CAN ALSO PROVIDE A 250-WORD (MAXIMUM) EXCERPT FROM A CASE STUDY FOR ANY OF THE ABOVE FEATURES THAT SHOWS HOW A CUSTOMER PUT A SOLUTION IN PLACE TO PROTECT THEIR BUSINESS, THIS WILL GET PRIORITY CONSIDERATION. A SUITABLE IMAGE SHOULD ALSO BE SUPPLIED.

DEADLINE REMINDER FOR ALL SUBMISSIONS: FRIDAY, 12 AUGUST, 2022

EMAIL ALL TEXT AND IMAGES TO EDITOR BRIAN WALL AT:
bp.wall@btinternet.com